製造 OT 向けのセキュリティのベストプラクティス

2021 年 *5* 月 *20* 日

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。このドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

目次

要約

クラウド、IoT、エッジコンピューティングでの新しい進歩に伴って、従来のオンプレミス製造のオペレーションテクノロジー (OT) ワークロードがハイブリッドワークロードへと生まれ変わる道が開けました。本書では、これらのオンプレミスハイブリッド製造ワークロードを AWS クラウド向けに設計、デプロイ、構築する際のセキュリティのベストプラクティスについて説明します。

はじめに

従来の製造ワークロードは、オペレーションテクノロジー (OT) ワークロードとインフォメーションテクノロジー (IT) ワークロードに分類できます。OT ワークロードは製造業務をサポートします。IT ワークロードは事業運営をサポートします。

OT ワークロードは、製造現場のオペレーションをサポートするため、通常は工場内に位置しています。しかし、クラウド、IoT、エッジコンピューティングの導入により、OT ワークロードはオンプレミスワークロードからハイブリッドワークロードへと変革を遂げ、クラウドサービスを活用できるようになりました。

本書では、分散型製造ワークロードを AWS クラウド向けに設計、デプロイ、構築する際のセキュリティのベストプラクティスについて説明します。 本書は、産業用のエッジコンピューティングでリソースを保護することに重点を置いています。クラウドのリソースを保護するためのベストプラクティスについては、AWS Well-Architected Framework のセキュリティの柱を参照してください。

次の図に示すように、製造ワークロードのクラウド統合ポイントとリソースの配置を定義する背景として Purdue モデルを使用します。Purdue モデルは、製造業界のリファレンスモデルであり、国際計測制御学会 ISA-95 規格の基礎として使用されており、製造と事業の統合に関する詳細な情報モデルを定義します。

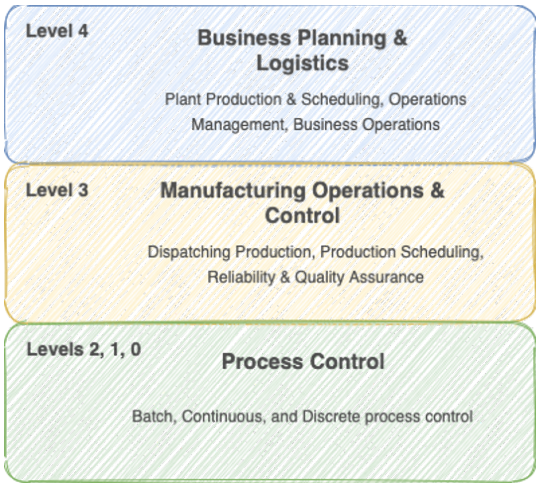

図 *1 - Purdue* エンタープライズのリファレンスアーキテクチャモデル

Purdue リファレンスモデルを産業用制御ネットワークに適用した場合の IT と OT の機能の配置は次の図に示すとおりです。

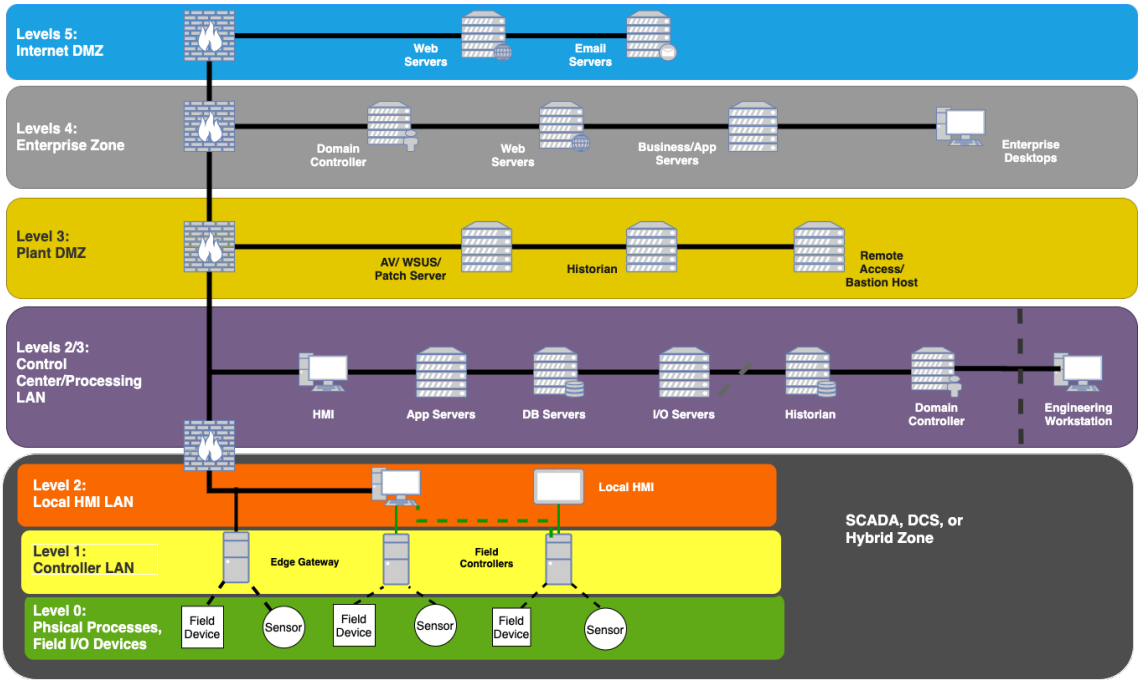

図 *2 - Purdue* モデルで表現した産業用制御ネットワーク

レベル 4 とレベル 5 は IT ドメインにあります。ほとんどの企業 (事業者) では、インターネット (レベル 5) との境界線にあたるエンタープライズネットワークは、レベル

4 のインフラストラクチャーが提供する事業運営とともに、伝統的に IT 組織によって管理されています。企業と AWS クラウドとの間の接続方法として最もよく使用されているのは、レベル 5 の DMZ ファイアウォールを介したインターネット接続です。

レベル 3 とレベル 4 との間のファイアウォールは、企業データバックボーンとローカルの産業用設備との間のインターフェイスです。レベル 3 以下で実装している機能は、製造業務および制御に関連しています。

レベル 2、レベル 1、レベル 0 は、いわゆるセル/エリアゾーンを構成します。レベル 2 には、HMI (Human Machine Interface)、SCADA (Supervisory Control and Data Acquisition)、DCS (Distributed Control System) が含まれており、レベル 1 のロジックコントローラーを介してレベル 0 の製造制御アセット (フィールドデバイスやセンサー) とやり取りするために使用します。

IoT テクノロジーを活用したコネクテッドセンサーやコントローラーの登場により、ローカルの HMI アセットで使用できる新しいゲートウェイデバイスが導入されました。ただし、これらは産業用のアセットとマシンデータをクラウドに送信するように意図的に設計されています。

運用効率を向上させるためのインサイトは、レベル 3、2、1 の MES (Manufacturing Execution Systems)、SCADA/DCS、PLC (Programmable Logic Controllers) などのサービスやアプリケーションで生成したデータから得られます。本書では、この点について重点的に説明します。このデータを効率的に処理するには、AWS クラウド内で利用できるオンデマンドのコンピューティングリソース、コスト効率の高い無制限のストレージ、分析および 人工知能/機械学習 (以下、AI / ML) サービスを活用します。

AWS および AWS のサービスに接続するには、AWS Direct Connect、AWS Virtual Private Network (AWS VPN)、AWS Transit Gateway など、さまざまな AWS のサービスを使用できます。OT レイヤーに必要な機能によっては、インターネット経由でクラウドに接続しても達成できないレベルのパフォーマンス (予測可能な低レイテンシ

ー、高帯域幅) を、AWS Direct Connect で達成できる場合があります。このような従来のオンプレミス OT ワークロードをクラウドに接続することを、ハイブリッド環境といいます。

シナリオ

次のシナリオでは、AWS のサービスを製造に使用する (または使用できる) 一般的なパターンを定義します。これらの一般的な使用パターンに関連するセキュリティ上の課題をより良く理解するために次のリストが役立ちます。これらの課題の検討から生じる疑問については、本書の「**セキュリティのベストプラクティス**」セクションで対応します。

製造データからインサイトを得る

製造業ではクラウドを採用して、企業全体にわたってスケールするデジタルイノベーションを実現し、クラウドを活用して製造データを総合的に分析してインサイトを抽出することを望んでいます。これらのユースケースに対応するには、AWS のクラウドサービスとエッジサービスを組み合わせることで、製造業にて現行およびレガシーのさまざまなシステムや機器からデータを取り込み、構造化し、保存して、コンテキストに基づき単一ソースとなるデータセットを作成できるようにします。このデータを活用することで、包括的な分析と利用が容易になり、事業運営のデジタルトランスフォーメーションと改善が可能になります。次の図は、ファクトリーデータからインサイトを取得する一般的なステップを示しています。

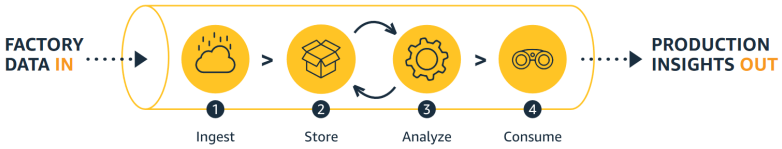

図 3 - データからインサイトへ

OT リソースからクラウドへのデータの抽出、構造化、取り込みは、データ分析を可能にする最初のステップです。AWS には、処理、分析、インサイト生成のためのさまざまな分析サービスがクラウド内にありますが、取り込みステージではハイブリッドコンポーネントと OT リソースとのやり取りが必要になります。OT 環境からクラウドへのデータの取り込み (レベル 1～3) を可能にする AWS の主要なサービスの一部を次に示しています。視覚的な表現については、「Manufacturing on AWS」のリファレンスアーキテクチャ図を参照してください。

- **AWS IoT Core** - MQTT を介して IoT デバイスからデータを取り込みます。
- **AWS IoT Greengrass** - MQTT、またはさまざまな組み込み/カスタムコネクターや AWS Lambda 関数を使用して、レガシーデバイスや IoT デバイスからデータを取り込みます。
- **AWS IoT SiteWise** - OPC UA、EtherNet/IP、Modbus、MQTT、または API コール経由で直接、マシンデータを収集、整理、分析します。
- **Amazon Kinesis** - ストリーミングデータを取り込みます。
- **Amazon CloudWatch** - ログとインフラストラクチャのメトリクスを取り込みます。
- **AWS Data Sync** - オンプレミスのファイルデータを取り込み、Amazon Simple Storage Service (Amazon S3) に同期します。
- **AWS Storage Gateway** - Amazon S3 にデータを取り込むためのローカルファイルサーバーとして機能します。
- **AWS Transfer for SFTP** - Amazon S3 にファイルを取り込むためのクラウド FTP サーバーとして機能します。
- **Database Migration Service** - オンプレミスデータベースをクラウドに移行または同期します。

AWS のサービスに加えて、サードパーティーとの統合やサードパーティーのサービスもデータ取り込みに利用できます。お客様は製造データをクラウドに取り込むための幅広いオプションから選択できます。

サービスごとに具体的なメカニズムは異なりますが、通常、これらのサービスのコンポーネントはエッジにデプロイします (ISA 95/Purdue モデルのレベル 3 以下)。これらのコンポーネントは、プロトコル変換、セキュアなクラウド接続、ローカルデータ変換、キャッシュなどのサービスを提供するための仲介役として機能します。

エッジでのデバイス制御/機械学習の推論

従来、製造業界はオンプレミスで実行する PLC や産業用ソフトウェア (SCADA/DCS/MES など) を使用して、デバイス制御やプロセスのオーケストレーション、またはオートメーションを行っていました。製造業界では、これらのローカル機能を強化するために、クラウドテクノロジーの導入を急速に進めています。

エッジでの AI / ML は、そのような強化策の 1 つです。AWS は、あらゆる組織が AI / ML に簡単にアクセスするために利用できる一連のツールを提供しています。製造業では、これらの高度なツールを活用して、プロセス制御の課題を解決できます。クラウドでモデルをトレーニングし、エッジにデプロイすることで、機械学習を高度なプロセス制御に活用できます。例えば、お客様は AI / ML でモニタリングする目視検査を追加して、不具合や例外の検出を改善できます。

AWS IoT Greengrass を使用したプロセスのオーケストレーションと制御は、ローカルの制御機能を強化するもう 1 つの方法です。AWS Lambda 関数と Docker コンテナで実行するマイクロサービスは、AWS IoT Greengrass によってデプロイできます。AWS IoT Greengrass では、コードの管理およびデプロイをクラウドから実行できる一元的な方法を提供します。大規模なコードを柔軟に管理できるため、オンサイトの専門家やサポートへの依存を減らすことができます。図 4 は、re:Invent セッショ

ンの「AWS IoT and Industrial Automation at Amazon」で示したプロセスオーケストレーションの例です。

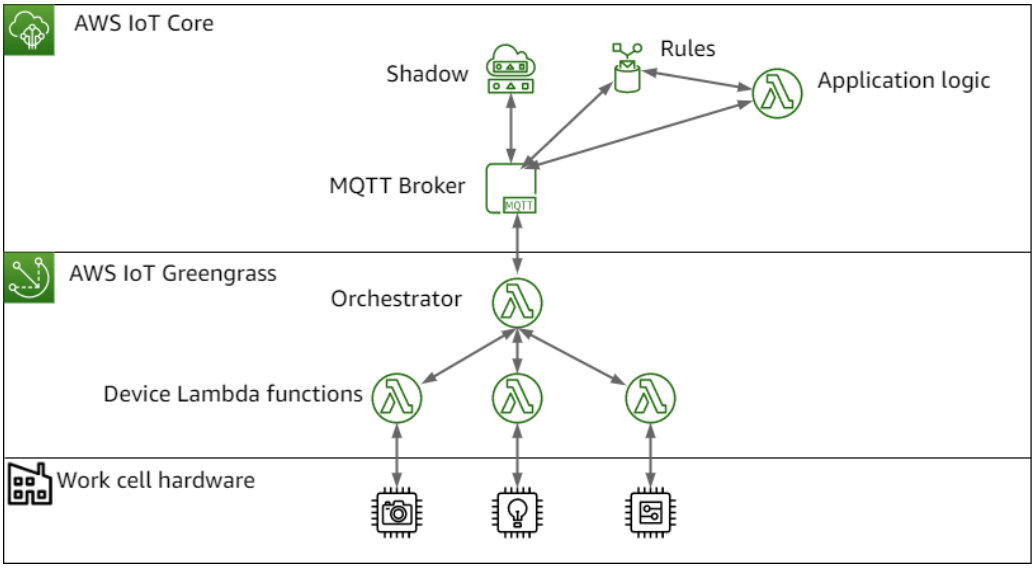

図 *4 - AWS IoT Greengrass* を使用したプロセスオーケストレーションの例

FreeRTOS は、ライブラリを組み込んだリアルタイムオペレーティングシステム (OS) で、AWS のサービスとのセキュアな接続を確立し、OTA (Over-the-Air Update) を可能にします。産業用制御タスクに最適であり、産業用のスマートセンサー、アクチュエーター、ポンプなどのコンポーネントの組み込みコントローラーとしても適しています。

このシナリオでは、クラウド対応コンポーネントを工場ネットワークのレベル 0～3 に配置できます。また、コントローラーに書き戻して、産業用機器を制御する機能を備えたこのシナリオでは、慎重なセキュリティの計画と実装が必要です。

エッジコンピューティングのインフラストラクチャの管理

一般的な製造用設備では、産業用データセンター、産業用 PC、ゲートウェイなど、オンプレミスのコンピューティングインフラストラクチャを管理する必要があります。このインフラストラクチャの管理は、ハードウェア/ソフトウェアが異なること、一元管

理インターフェイスがないこと、ベストプラクティスを簡単に導入できないことなどが原因で、課題となる場合があります。このインフラストラクチャに関する責任は、OT ドメインと IT ドメインとの間で共有します。お客様は、IT インフラストラクチャの管理のベストプラクティスに従い、AWS Systems Manager や Amazon CloudWatch などのオンプレミスの管理およびモニタリングサービスを活用することで、AWS のエクスペリエンスを活用できます。これらのサービスを利用すると、クラウドのリソースと同様の方法で、大規模なオンプレミスのインフラストラクチャを管理できます。これにより、オンプレミスでベストプラクティスを導入する際の障壁が取り除かれます。

例えば、Amazon CloudWatch エージェントを使用して、製造アプリケーションを実行しているエッジサーバーのヘルスチェック/使用状況のメトリクスやログをモニタリングできます。お客様は、障害や例外が発生した場合に通知を受け取るようにアラートを設定できます。AWS Systems Manager は、デバイスの一元管理に使用できます。お客様は、ソフトウェアインベントリ、オペレーションシステムのバージョン、インストール済みのパッチを収集できます。また、ソフトウェアのインストールやパッチ管理などのタスクを自動化できます。これにより、指定したパッチ、設定、カスタムポリシーに対してインスタンスをスキャンすることで、セキュリティとコンプライアンスの要件を維持することもできます。

一方、AWS Outposts は、ユーティリティコンピューティングをエッジまで拡張するフルマネージドサービスを提供します。このサービスは、他のクラウド設備と同様に、AWS マネジメントコンソール、SDK、API で管理し、お客様の設備にデプロイします。このサービスは、オンプレミスのインフラストラクチャの管理とガバナンスをシンプルにし、ベストプラクティスの導入に伴う障壁を取り除くように設計されています。クラウドサービスのパワーを活用して、既存のインフラストラクチャを強化し、オンプレミスとクラウドの境界を取り除きます。

統合生産

企業ワークロードで AWS クラウドを利用した経験があるお客様は、すべてのワークロードで同様のエクスペリエンスを得たいと強く希望します。AWS for the Edge は、ユーティリティコンピューティングをクラウドデータセンターの外に広げるように設計された一連のサービスやテクノロジーです。これらのテクノロジーを利用することで、お客様はすべての製造および IT ワークロードで同じ一貫したエクスペリエンスを実現できます。

AWS for the Edge は、次のソフトウェアコンポーネントで構成されています。

- **FreeRTOS** - マイクロコントローラー用のオペレーティングシステムであり、AWS IoT に接続する小型で低電力のエッジデバイスを構築できます。
- **AWS IoT SiteWise** - 産業用機器から大規模なデータを簡単に収集、整理、分析できます。
- **AWS IoT Greengrass** - AWS をエッジデバイスまで拡張し、生成したデータをローカルに処理しながら、クラウドを使用して管理、分析、保存を継続できるようにします。
- **Alexa Voice Service (AVS) の統合** - AWS IoT Core の機能であり、デバイスメーカーは任意の接続されているデバイスを Alexa の組み込みデバイスにすることができます。
- **Amazon Kinesis Video Streams** - 再生、分析、機械学習のためのメディアストリームをキャプチャ、処理、保存します。
- **Amazon SageMaker Neo** - 機械学習モデルを一度トレーニングするだけで、クラウド内やエッジ内のどこででも実行できるようにします。

- **AWS RoboMaker** - クラウド規模でロボットアプリケーションをシミュレートし、デプロイします。

AWS for the Edge は、クラウドのハードウェア拡張のための次のオプションも提供しています。

- **AWS Snowcone** - ポータブルで頑丈な小型のエッジコンピューティングおよび転送デバイス。
- **AWS Snowball** - Amazon EC2 とストレージを搭載した、頑丈で出荷可能なエッジコンピューティングプラットフォーム。
- **AWS Outposts** - AWS インフラストラクチャおよびサービスをオンプレミスで実行し、真に一貫したハイブリッドエクスペリエンスを実現します。
- **AWS Wavelength** - AWS Wavelength は、モバイルエッジコンピューティングアプリケーション向けに最適化された AWS インフラストラクチャサービスです。
- **AWS Storage Gateway** - AWS Storage Gateway は、実質的に無制限のクラウドストレージにオンプレミスからアクセスできるハイブリッドクラウドストレージサービスです。

クラウドコンピューティングは、レベル 4～5 の製造アプリケーションの移行とモダナイゼーションに推奨されるプラットフォームです。これらの製造アプリケーションには、生産計画、エンタープライズリソースプランニング (ERP)、製品ライフサイクル管理 (PLM)、ハイパフォーマンスコンピューティング (HPC)、コンピュータ支援設計 (CAD)、産業用データレイクなどが含まれます。エッジコンピューティングは、モダナイゼーションの拡張を MES や SCADA、IIoT (Industrial Internet of Things)、増えつつある産業用モノ (Thing) や産業用コンピュータ (IPC) の管理まで及ぼします。

企業の製造業では、産業用設備を企業の他の部分に接続することで、グローバルな規模で業務へのより深いインサイトを取得し、各リーダーやマネージャーに相応の継続的なガイダンスを提供できます。製造現場で生成および利用される双方向の情報フローにより、統合製造と呼ばれる新しいレベルの総合的な効率化を実現できます。

セキュリティ原則

オンプレミスの OT セキュリティに関する次の主要なセキュリティ原則は、AWS Well-Architected Framework のセキュリティの柱の設計原則、ICS サイバーセキュリティに関する NIST ガイドライン、ゼロトラストアーキテクチャに関する NIST ガイドライン、IEC 62443 規格シリーズに適合しています。これらは、ハイブリッド製造環境の課題に合わせて適応および拡張されています。また、ハイブリッド製造環境のセキュリティについて検討する際に適用する、一連の主な基本的ガイドラインを提供します。

- **すべての通信をセキュリティで保護する** - ネットワークの場所だけでは、信頼を確保できません。従来、OT 環境はエアギャップされたシステムであり、これらのネットワークの主要な防御メカニズムとして境界セキュリティを使用しています。そのため、ネットワーク境界内のリソースは「信頼できる」と見なされ、セキュリティメカニズムを一切使用していません。この原則では、ネットワークの境界内または境界外を問わず、すべての通信をできるだけセキュアな方法で行い、ソース認証を提供し、機密性と整合性を保護する必要があることを定めています。ネットワークセグメンテーションや分離 (セル/ゾーン/エリアセグメンテーションなど) の既存の方法も含めて、ゼロトラスト原則を適用することで、これらの従来の信頼境界を狭め、ネットワークの場所への依存を減らすことができます。

- **トレーサビリティを有効にする** - トレーサビリティは、セキュアな産業用ネットワークの維持と運用に不可欠です。企業は、環境に対するアクションと変更をリアルタイムでモニタリング、アラート、監査する必要があります。アセットインベントリ (ハードウェアとソフトウェア)、ネットワークトラフィック、アクセスリクエスト、関連するログとメトリクスに関するデータを収集する必要があります。これらのデータ収集システムは、自動的に調査して対処できるように、システムと統合する必要があります。また、データを分析して、ポリシーの作成と適用を改善するためのインサイトを得る必要があります。
- **伝送中および保管中のデータを保護する** - データを保護するために、データを複数の機密性レベルに分類し、必要に応じて暗号化、トークナイゼーション、アクセスコントロールなどのメカニズムを使用します。データの分類は、製造業界では (金融業界やヘルスケア業界と比べて) 一般的ではありませんが、データの種類によっては特に精査を要することが重要なポイントです。データ損失防止 (バックアップ、冗長性、災害対策など) も、データの保護とセキュリティ確保の一環です。
- **すべてのレイヤーでセキュリティを適用する** - 複数のセキュリティコントロールを使用して多層防御 (defense in-depth) アプローチを適用します。すべてのレイヤーでセキュリティを適用します (例: AWS クラウド内の VPC、エッジネットワーク、OT ネットワーク、コンピューティングインスタンス、オペレーティングシステム、アプリケーション、コードなど)。

セキュリティのベストプラクティス

次のベストプラクティスは、リスクの評価および軽減戦略を通じてビジネス価値を提供しつつ、情報、システム、アセットを保護するためのガイドラインです。製造を行う機関は、強力なサイバーセキュリティ体制を維持する必要があります。セキュリティのベ

ストプラクティスは、規範的なアプローチを採用して、使用シナリオの各課題領域にソリューションを推奨し、ハイブリッド製造環境の保護という課題に対処することです。

図 5 は、製造 OT でのセキュリティのベストプラクティスを示すリファレンス図です。この図は、本書の以降のセクションでベストプラクティスを示すための視覚的な補助として使用します。

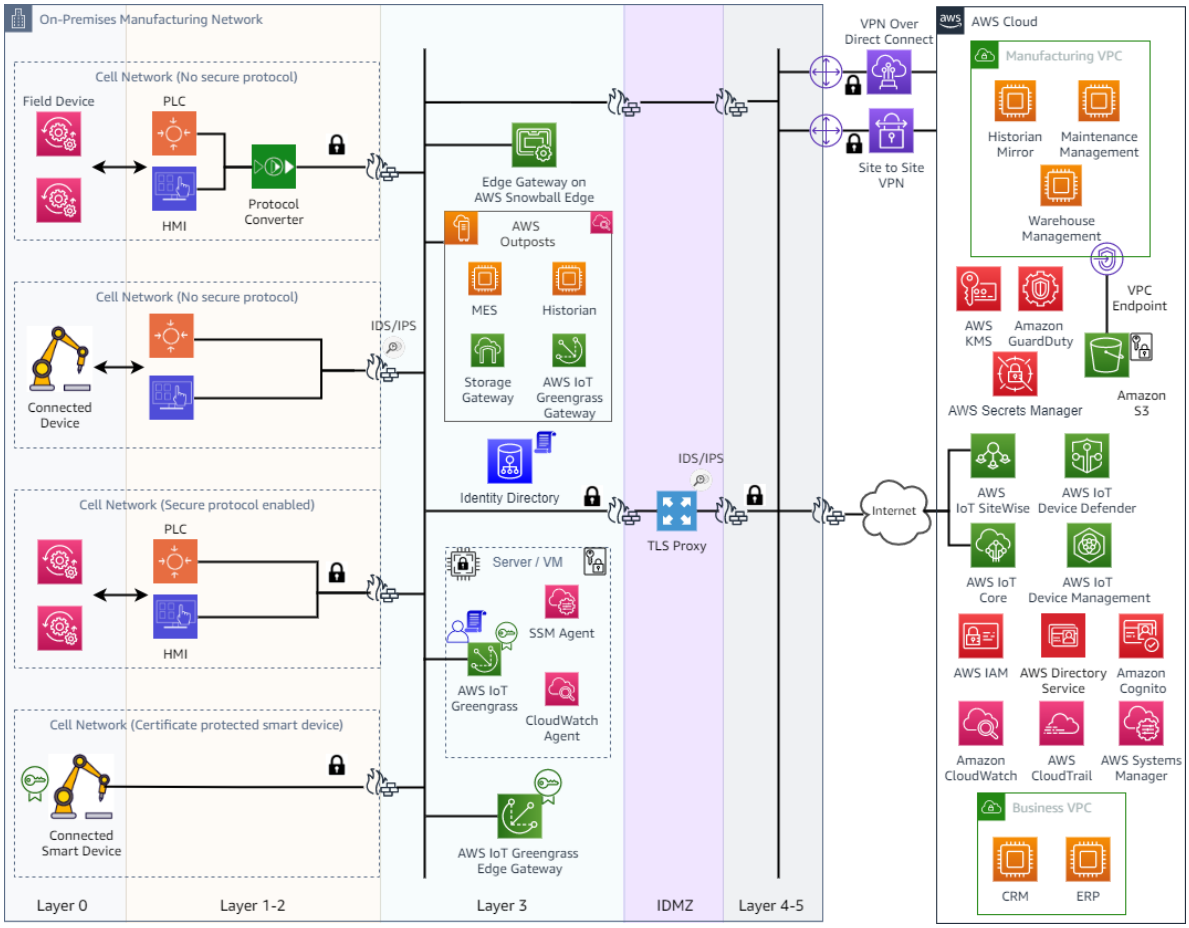

図 5 - 製造 OT でのセキュリティのベストプラクティスを示すリファレンス図

クラウドへのセキュアなネットワーク接続

セキュアなクラウド接続を管理するベストプラクティスは、ネットワークトラフィックをプライベートかつ暗号化された状態に保つことです。ネットワークトラフィックを AWS VPN またはプライベートネットワーク経由でルーティングできず、インターネ

ット経由でクラウドサービスに直接アクセスする必要がある場合は、トラフィックを暗号化し、TLS プロキシとオンプレミスのファイアウォールを介してルーティングすることで、保護を強化する必要があります。図 6 は、これらのベストプラクティスの一部を示しています。

- **AWS Site-to-Site VPN または AWS Direct Connect 経由で AWS とのセキュアな接続を確立する** - AWS には、製造エッジから AWS 環境へのセキュアな接続を確立するための複数の方法と設計パターンが用意されています。パブリックインターネット経由で AWS へのセキュアな AWS VPN 接続を確立するか、AWS Direct Connect 経由で専用のプライベート接続をセットアップします。AWS Direct Connect で AWS VPN を使用して、AWS Direct Connect 経由でトラフィックを暗号化することも可能です。

- **可能な場合は VPC エンドポイントまたは VPC エンドポイントサービスを優先する** - パブリックインターネットによる AWS VPN、もしくは AWS Direct Connect 経由で AWS へのセキュアな接続を確立したら、可能な限り、VPC エンドポイントを使用します。VPC エンドポイントを使用すると、パブリック IP アドレスを必要とせずに、サポートされているリージョンのサービスにプライベートに接続できます。エンドポイントは、エンドポイントポリシーもサポートしています。これにより、必要なリソースのみへのアクセスを制御および制限できます。

  VPC エンドポイントサービス (AWS PrivateLink) を使用すると、クラウド内の Amazon VPC で独自のアプリケーションを作成し、これを VPC エンドポイントとして設定できます。

- **パブリックインターネット経由で AWS に接続するサービスに TLS プロキシとファイアウォールを使用する** - 必要なサービスの VPC エンドポイントが利用できない場合は、パブリックインターネット経由でセキュアな接続を確立する必要

があります。このようなシナリオのベストプラクティスは、これらの接続を TLS プロキシとファイアウォールを介してルーティングすることです。

次の図は、プロキシ経由でクラウドに接続した AWS IoT Greengrass のゲートウェイの例を示しています。プロキシを使用すると、クラウドトラフィックの検査とモニタリングが可能になり、脅威とマルウェアを検出できます。また、セキュリティポリシーをネットワークレイヤーで適用することもできます。ファイアウォールルールを HTTPS および MQTT トラフィックに対して設定する必要があります。ネットワーク接続が断続的に失われるのを防ぐために、ゲートウェイは AWS IoT Greengrass Stream Manager などの「ストアアンドフォワード」方式を使用して、接続が復元されるまでデータをローカルにバッファすべきです。

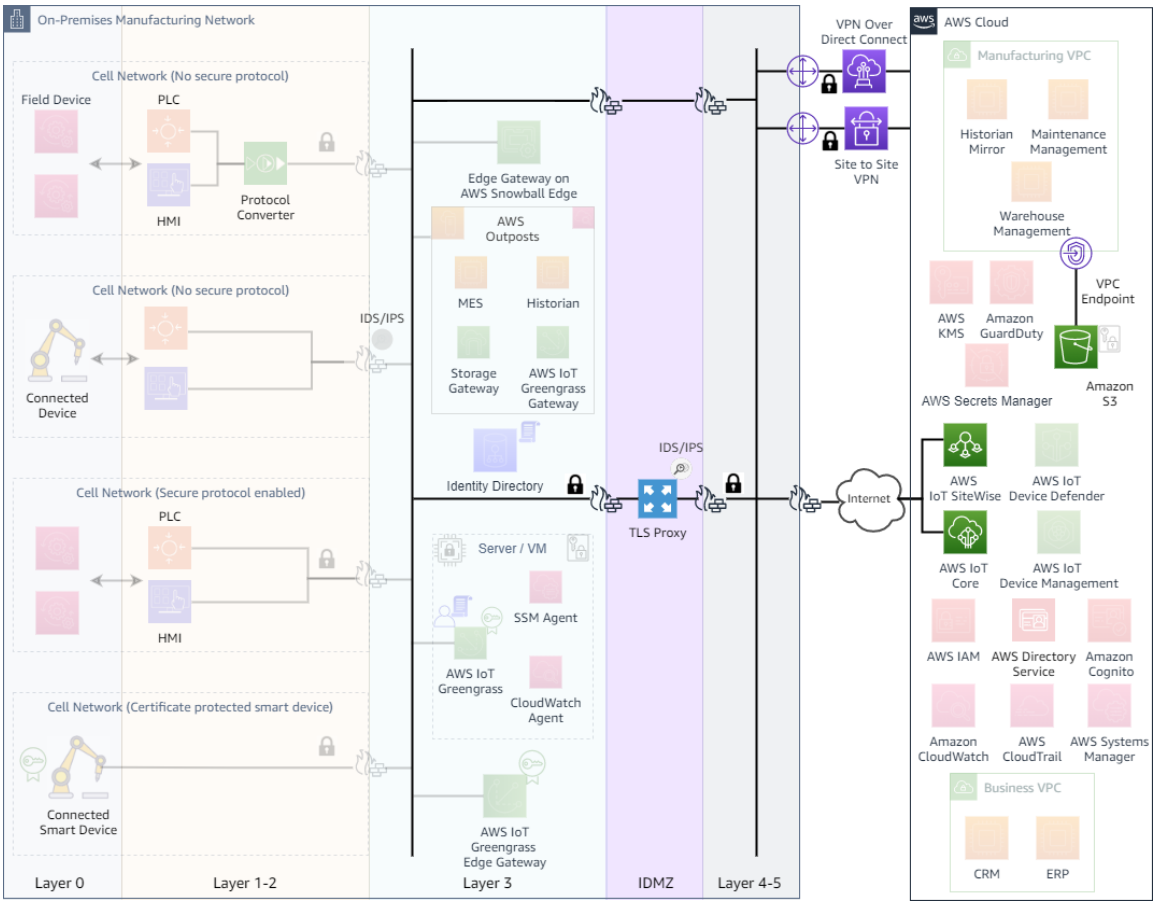

図 6 - クラウドへのセキュアなネットワーク接続

ローカルリソースへのセキュアなネットワーク接続

AWS クラウドで実行する製造アプリケーション、またはクラウドに接続したオンプレミスエッジゲートウェイで実行するアプリケーションは、PLC やフィールドデバイスなどのローカルネットワークリソースにアクセスする必要があります。これらのネットワークリソースには、ローカルコンピュータ (HMI/SCADA)、ファイルシステム、またはデータベースが含まれる場合もあります。製造環境は、多くの場合、ローカルネットワークリソースの暗黙的な信頼を前提として動作します。エッジゲートウェイやエージェントソフトウェアをローカルネットワークの一部として使用することはできますが、これらは信頼できないものと見なして、セキュアな方法で他のリソースとの接続を確立する必要があります。これらのベストプラクティスの一部を次に示します。

- **セキュアな産業用プロトコルを使用する** - 従来、産業用制御システム (ICS: Industrial Control Systems) は、エアギャップされたシステム (分離環境) であり、独自の制御プロトコルを実行しています。これらの ICS プロトコルは、何十年もの間、製造業界の困難なニーズに対応してきました。しかし、これらのプロトコルは、すべての通信が信頼できる環境で行われていることを前提として設計されており、主に境界セキュリティに依存していました。そのため、ICS プロトコルは通常、暗号化、認証、認可のセキュリティ要件をサポートしていませんでした。

  しかし、産業用サイバーセキュリティに対する意識が高まり、スマートファクトリーやクラウドコネクテッドシステムへの進化が深まる中、セキュアな通信をサポートするための新しいバージョンの ICS プロトコルが開発されています。既存のセキュアなバージョンの産業用プロトコルの例をいくつか次に示します。

  - **CIP Security** - これは、CIP (Common Industrial Protocol) データをプロトコルレベルで保護する新しい方法です。CIP は、数百のベンダーがサポートする産業用プロトコルです。CIP Security は、認証、メッセージの

整合性の検証、暗号化の仕様を CIP プロトコルに追加し、セキュリティを確保します。

- **Modbus Secure** - この新しいプロトコルは、TLS (Transport Layer Security) と、一般的な産業用プロトコルである従来の Modbus プロトコルをブレンドすることで、堅牢な保護を提供します。この新しいプロトコルでは、サーバーとクライアントの認証に X.509 v3 デジタル証明書を利用しています。このプロトコルは、X.509 v3 拡張機能を使用したロールベースのアクセスコントロール情報の送信もサポートし、クライアントのリクエストを承認します。
- **OPC UA** – OPC (Open Process Communications) は、業界における相互運用標準です。OPC UA は OPC の最新版であり、セキュアな設計のクロスプラットフォームです。X.509 証明書と、ユーザー認証情報ベースの認証および認可スキームの組み合わせを提供します。また、伝送中のデータ暗号化も提供します。OPC UA 仕様では、サーバー主導の接続 (リバース接続) も可能です。これにより、クライアントはインバウンドファイアウォールポートを開かずにサーバーと通信できます。

  ベストプラクティスは、セキュアなバージョンのプロトコルを使用することです。ベンダーサポートが利用できない場合は、既存のコントロールシステムアーキテクチャをアップグレードまたはアップフィットして、セキュアなプロトコルサポートを有効にすることを検討してください。

- **信頼境界を強化する** - ICS の領域におけるセキュアなプロトコルはかなり新しいものであり、これらのプロトコルに対するベンダーサポートはさまざまです。新しいプロトコルへのアップフィットやアップグレードができない場合は、信頼境界を狭めることを検討してください。例えば、セキュアでない通信の範囲と領域を制限します。信頼境界を狭める 1 つの方法は、通信を変換および保護でき

るプロトコルコンバーターをできるだけコントローラー (データソース) の近くに配置することです。この場合、コントロールパネル内に直接配置するプロトコルコンバーター PLC モジュールを利用できます。

別の推奨事項は、工場を複数のセル/エリアゾーンに分離する (機械工場、塗装ブース、部品組立などの機能領域別に ICS デバイスをグループ化する) ことです。このシナリオの場合、セル/エリアゾーンが定義する信頼境界では、デバイスが妨げられずにリアルタイムで通信できますが、セル/エリアゾーンに出入りするトラフィックは検査の対象となります (図 7 を参照)。ICS プロトコルを理解して制御ネットワークの異常な動作を検出できる ICS 専用のファイアウォール/検査製品を使用することを検討してください。

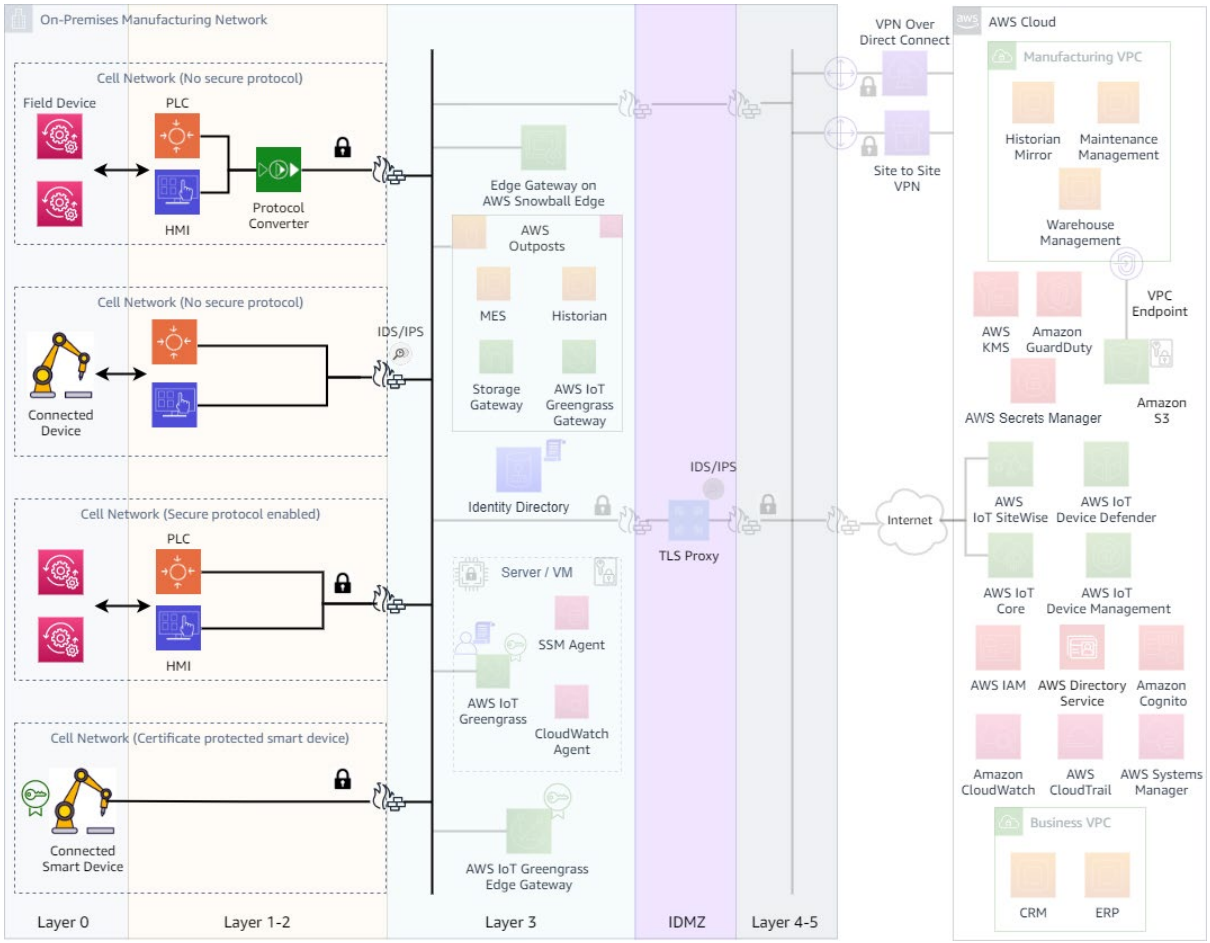

図 7 - ローカルリソースへのセキュアな接続

クラウドにセキュアに接続されたネットワークリソース

エッジゲートウェイ、エージェントソフトウェア、IoT デバイスなど、クラウドに接続されたネットワークリソースは、予期せぬアクセスのリスクを軽減するために強化する必要があります。また、クラウドに接続されたリソースからローカルリソースにアクセスするための認証情報とアクセス許可を管理して、有害事象の影響範囲を制限する必要があります。図 11 - 図 12 は、これらのベストプラクティスの一部を示しています。

- **クラウドに接続したコンピューティングリソースを強化する** - エッジゲートウェイのオペレーティングシステムごとに個別のハードニングのガイドラインは異なりますが、一般的なガイドラインとしては、OS を堅牢化してセキュアに設定します。
    - 不要なサービス、アプリケーション、ネットワークプロトコルを削除します。
    - OS ユーザー認証を設定します (不要なアカウントの削除、非インタラクティブなアカウントの無効化、時刻の自動同期の設定を行います)。
    - リソースコントロールを適切に設定します (必要なリソースにのみアクセスを許可します)。
    - 追加のセキュリティ制御 (マルウェア対策、侵入検出、ホストベースのファイアウォール) をインストールして設定します。

    USB やシリアルなどの不要なハードウェアポートへのアクセスも、物理手段とソフトウェア手段の両方を使用して無効にする必要があります。

    エッジゲートウェイをベンダーから購入すると、OS に直接アクセスできない場合があります。ベンダーのドキュメントを参照して、基盤となる OS を強化するための適切なステップをベンダーが実行していることを確認してください。

- **TPM などのハードウェアセキュリティ機能を使用してデバイスを保護する** - Trusted Platform Module (TPM) などのハードウェアセキュリティ機能をできるだけ活用します。TPM は、ほとんどの商用 PC およびサーバーに備わっている暗号化プロセッサです。至るところで TPM は活用でき、VPN アクセス用のキーやハードディスク用の暗号化キーを保存したり、プライベートキーの取得を目的とした辞書攻撃を防止したりなど、幅広いユースケースに使用できます。

  AWS IoT Greengrass では、プライベートキーのセキュアな保存とオフロードのためのハードウェアセキュリティモジュール (HSM) の使用をサポートしています (図 8 を参照)。プライベートキーは、HSM、TPM、その他の暗号化要素などのハードウェアモジュールにセキュアに保存できます。この機能に適合したデバイスについては、AWS Partner Device Catalog を参照してください。

  標準インストールでは、AWS IoT Greengrass で 2 つのプライベートキーを使用します。1 つのキーは、AWS IoT Greengrass Core を AWS IoT Core に接続するときに、Transport Layer Security (TLS) ハンドシェイク中の AWS IoT クライアント (IoT クライアント) コンポーネントで使用します (このキーは、コアプライベートキーとも呼ばれます)。 もう 1 つのキーは、ローカル MQTT サーバーで使用し、AWS IoT Greengrass デバイスが AWS IoT Greengrass Core と通信できるようにします。ハードウェアセキュリティは、共有または個別のプライベートキーを使用して、両方のコンポーネントに適用できます。詳細については、「AWS IoT Greengrass ハードウェアセキュリティに関するプロビジョニング慣行」を参照してください。

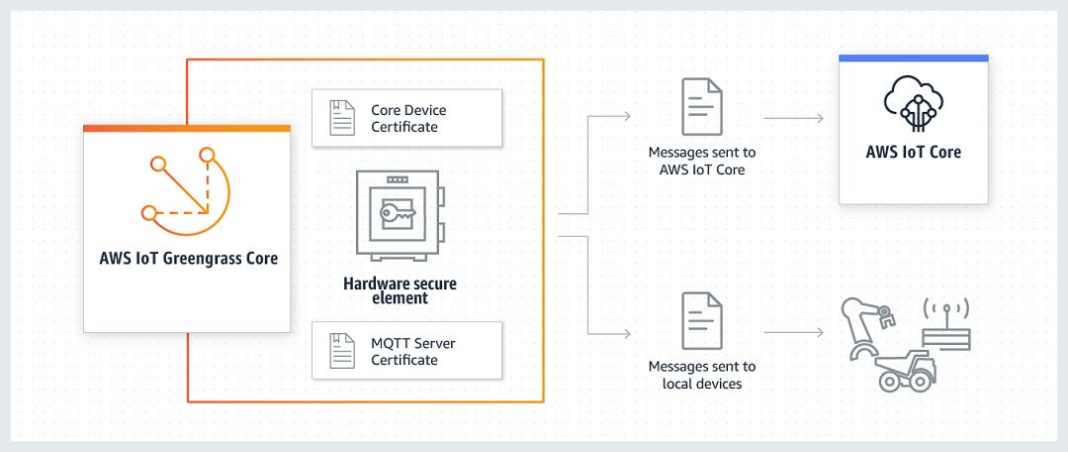

図 *8 - AWS IoT Greengrass* のハードウェアセキュリティアーキテクチャ

- **デバイスのセキュリティライフサイクルを計画および管理する** - 設計時にデバイスとソリューションのセキュリティライフサイクルを計画すると、ビジネスリスクを軽減し、インフラストラクチャのセキュリティ分析を前もって実行できます。

  デバイスのセキュリティライフサイクルにアプローチする方法の 1 つは、サプライチェーン分析です。直接的または間接的を問わず、多数のサプライヤーがデバイスのサプライチェーンに関与している場合があります。ソリューションの存続期間と信頼性を最大化するには、正規のコンポーネントを受け取っていることを確認します。

  ソフトウェアもサプライチェーンの一部です。サプライチェーン内の各ソフトウェアプロバイダーを分析して、サポートを提供しているかどうかと、パッチの配信方法を確認します。ファームウェア、パッチ、その他のソフトウェアを検証して信頼性と有効性を確認する計画を策定します。

- **IAM 認証情報よりも IAM ロール/デバイス証明書を優先する** - エッジソフトウェアでは、AWS リソースにアクセスするために AWS 認証情報が必要です。サービスに応じて、デバイスでは IAM ロール、X.509 証明書、アクセスキー、またはカスタム認証方法を使用できます。ハードコードした長期の認証情報 (アク

セスキー) を使用せずに、IAM ロールまたは X.509 証明書を認証に使用することを優先します。

AWS IoT の場合、デバイスは X.509 証明書または Amazon Cognito ID を使用してセキュアな TLS 接続経由で接続できます (図 10 を参照)。研究開発時や、一部のアプリケーションで API コールを行ったり、WebSockets を使用したりする場合は、IAM ユーザーやグループ、またはカスタム認証トークンを使用して認証を行うこともできます。カスタム認証を使用する場合、カスタムオーソライザーは、デバイスを認証し、AWS IoT または IAM ポリシーを使用してデバイスに指定されたアクセス許可を付与または拒否を実行する役割を担います。

各デバイスに一意の ID を割り当てて、デバイスまたはデバイスのグループごとにアクセス許可を管理する必要があります。デバイス証明書または静的な認証情報を使用する場合は、現在のベストプラクティスに従って、これらの認証情報を適切にローテーションする必要があります。

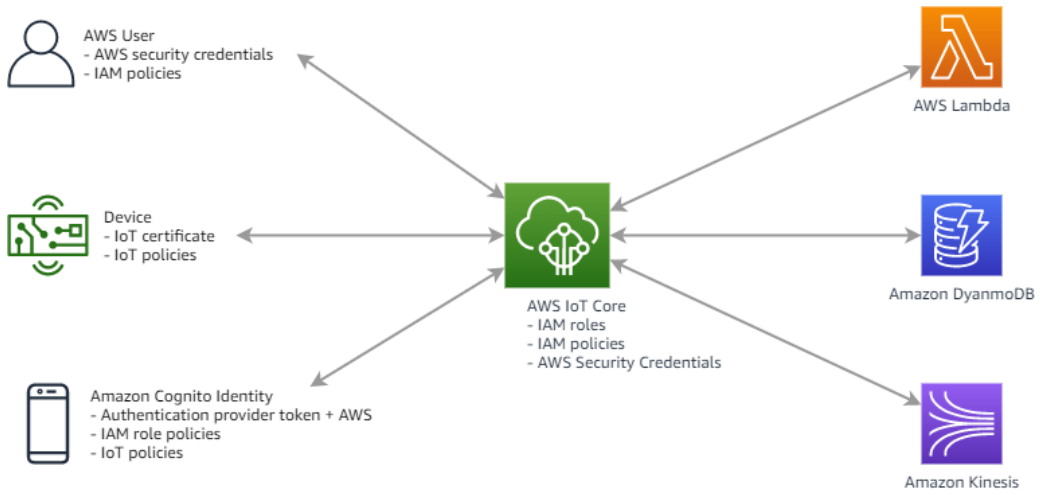

図 *9 - AWS IoT* の認証と認可

- **AWS IoT、AWS IoT Greengrass Core、AWS IoT Greengrass 対応デバイスの証明書ローテーションを実装する** -AWS IoT、AWS IoT Greengrass

Core、AWS IoT Greengrass 対応デバイスで使用する X.509 証明書は、ユーザーネームとパスワード、ベアラートークンなどの他のスキームよりも強力なクライアント認証を提供します。プライベートキーはデバイスから離れることがないためです。サーバー証明書が有効で期限切れになっていないことを確認するために、デバイスの時計が使用されます。したがって、デバイスでは正確な時刻を維持することが重要です。

きめ細かなクライアント管理アクション (証明書の失効など) を有効にするには、各デバイスやクライアントに一意の証明書を付与する必要があります。デバイスやクライアントは、証明書の有効期限が切れた場合や予期せず開示した場合に円滑な動作を確保するために、証明書のローテーションや置換もサポートする必要があります。

次の状況では証明書をローテーションします。

- 証明書の有効期限が切れる直前
- AWS IoT Device Defender で違反を検出した場合
- 不注意で開示した場合

例えば、AWS IoT Device Defender の監査を使用して、デバイス証明書が間もなく期限切れになるかどうかを確認できます。この報告を受け取った Amazon SNS トピックでは AWS Lambda 関数をトリガーし、証明書をローテーションするように AWS IoT のジョブをスケジュールします。

AWS IoT Greengrass に接続されたデバイスは、AWS IoT Greengrass Core のデバイスとの相互認証にローカル MQTT サーバー証明書を使用します。デフォルトでは、この証明書は 7 日後に失効します。この制限期間は、セキュリティのベストプラクティスに基づいています。MQTT サーバー証明書は、クラウドに保存されているグループ CA 証明書によって署名されます。有効期限は、

最大 30 日間に直接設定できます。AWS サポートに連絡してさらに長い期間に設定することもできます。ローテーションの回数を増やすと、クラウド接続の必要回数も増えます。ローテーション回数を減らすと、セキュリティ上の懸念が生じる可能性があります。証明書は手動でローテーションすることもできます。お客様は、各自のニーズに合った証明書ローテーションポリシーを作成して従う必要があります。

- **ローカル認証情報のハードコーディングや保存を避ける** - エッジソフトウェアでは、データベース、OPC UA サーバーなどのローカルリソースにアクセスするために認証情報が必要になる場合があります。認証情報をローカルに保存して管理する代わりに、AWS Secrets Manager などのセキュアなボールトストア (データ保管庫) 内に認証情報を保存します。AWS Secret Manager は、クラウド内にシークレットをセキュアに保存して管理するサービスです。コードは、API コールを介してシークレットを取得できます。AWS Secrets Manager は、認証情報を自動的に更新およびローテーションするように設定することもできます。シークレットは、選択した AWS Key Management Service (KMS) キーで暗号化します。管理者は、ロールやユーザーごとのきめ細かな IAM ポリシーを使用して、これらのシークレットへのアクセスを明示的に許可できます。

  AWS IoT Greengrass には、AWS Secrets Manager との統合が組み込まれています。AWS IoT Greengrass は AWS Secrets Manager を AWS IoT Greengrass Core のコアデバイスに拡張し、コネクタや AWS Lambda 関数がローカルシークレットを使用してサービスやアプリケーションと対話できるようにします。例えば、Twilio 通知コネクタは、ローカルに保存された認証トークンを使用します。シークレットを AWS IoT Greengrass グループに統合するには、AWS Secrets Manager のシークレットを参照するグループリソースを作成します。このシークレットリソースは、クラウドシークレットを ARN で参照します。シークレットリソースを作成、管理、使用する方法については、「シー

クレットリソースの使用」を参照してください。AWS IoT Greengrass は、伝送中および保管中のシークレットを暗号化します。グループのデプロイ時に、AWS IoT Greengrass は AWS Secrets Manager からシークレットを取得し、暗号化されたローカルコピーを AWS IoT Greengrass Core に作成します。AWS Secrets Manager でクラウドシークレットをローテーションした後で、グループを再デプロイして、更新した値を AWS IoT Greengrass Core に伝達します。図 10 は、シークレットを AWS IoT Greengrass Core にデプロイするプロセスの概要を示しています。シークレットは伝送中と保管中に暗号化されます。

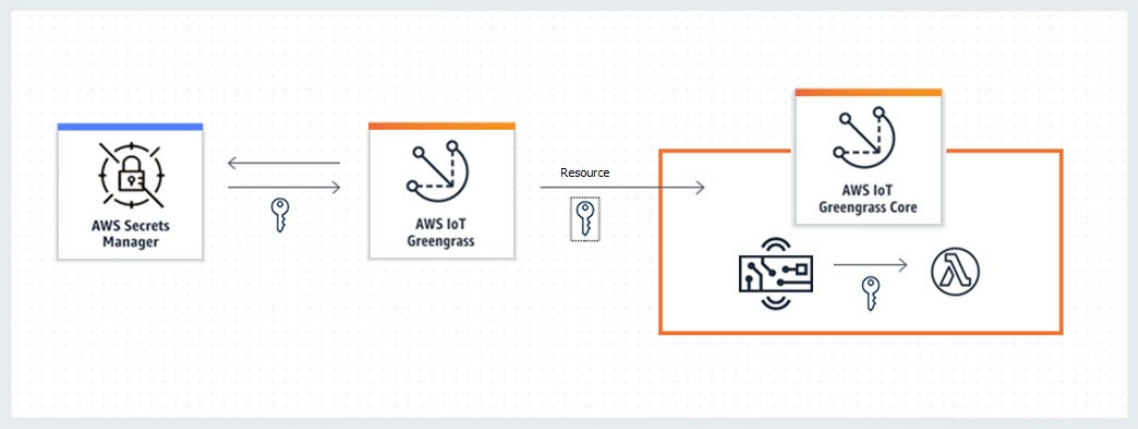

図 *10* - シークレットを *AWS IoT Greengrass Core* にデプロイする

- **ローカルリソースおよび AWS リソースにアクセスする「エッジゲートウェイ」と「エージェントソフトウェア」の最小権限アクセスコントロールを確保する** - エッジゲートウェイとエージェントソフトウェアは、ローカルリソースと AWS リソースの両方に対する必要なアクセスのみを許可するように設定する必要があります。エッジゲートウェイの場合、ローカルリソースへのアクセスは南側 (フィールドデバイス側) にあるファイアウォールを介して制御し、必要なローカルリソースへのアクセスのみに制限する必要があります (必要な PLC/OPC サーバー、IP アドレス、プロトコルへのアクセスのみなど)。OS / Active

Directory の許可を使用して、ファイルサーバーなどのローカルネットワークリソースへのアクセスも防ぐ必要があります。

エージェントソフトウェアは、多くの場合、ホストマシンにインストールし、収集するデータを生成します。ホストマシンリソースへのエージェントソフトウェアのアクセスを制限するには、オペレーティングシステムのアクセスコントロールを使用する必要があります。エージェントソフトウェアデーモン (またはサービス) は、必要な許可のみを持つそれ自身のユーザーアカウントで実行する必要があります。エッジゲートウェイと同様に、ファイアウォールと OS / Active Directory の許可を使用して、ローカルネットワークリソースへのアクセスを防止する必要があります。

AWS リソースへのアクセスは、エッジゲートウェイにアタッチされた適切な IAM ポリシー、またはエージェントソフトウェアの AWS アイデンティティ/ロールを使用して制御する必要があります。AWS Systems Manager と AWS Config を使用すると、OS 設定、システムレベルの更新、インストール済みのアプリケーション、ネットワーク設定などの変更を可視化して追跡できます。

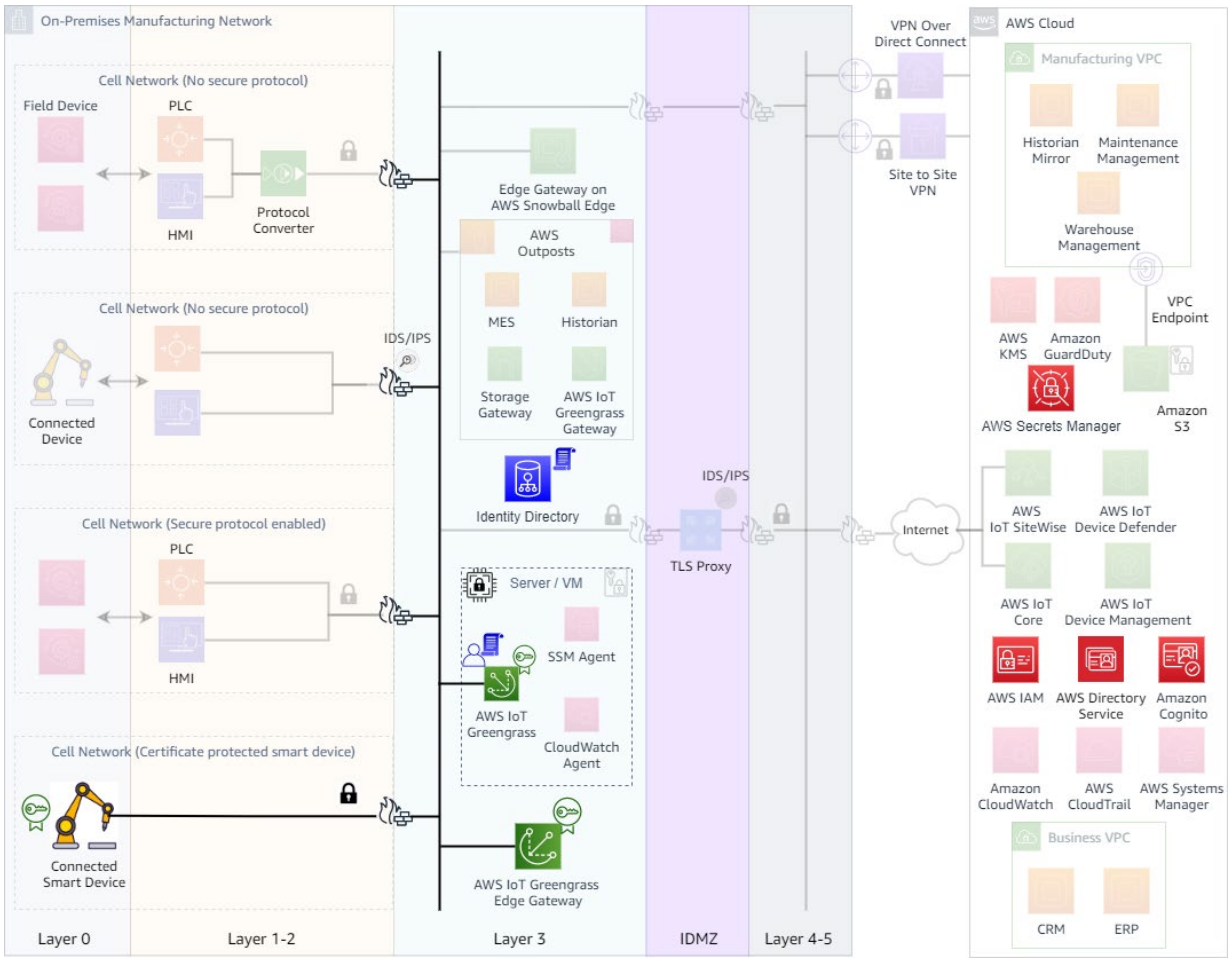

図 *11* - クラウドにセキュアに接続されたネットワークリソース

コンピューティングリソースをセキュアに管理してアクセスする

コンピューティングリソースを最新の状態に維持し、設定と管理のためにセキュアにアクセスし、変更を自動的にデプロイすることは、困難を伴う場合があります。この問題は、コンピューティングに異種のハードウェアやソフトウェアシステムを使用していると悪化し、ベストプラクティスを一貫して適用することが難しくなります。多くの場合、これに伴って必要以上に広い権限となり、セキュリティの脅威にさらされる機会が増えます (例えば、エッジゲートウェイをリモートで管理する従来のアプローチでは、

通常、RDP または SSH のポートを解放したり、あるいは VPN ソリューションに対応するため、ゲートウェイのセキュリティリスクが高まります)。AWS ではセキュアにリソースの管理を行うためのオプションを提供しており、既存のコンピューティングリソース (AWS System Manager) や IoT リソース (AWS IoT Device Management、AWS IoT Greengrass) を対象としています。また、すべてのリソースにベストプラクティスを一貫して簡単に適用できるフルマネージド型のインフラストラクチャサービス (AWS Outposts) もあります。図 12 は、これらのベストプラクティスの一部を示しています。

- **AWS Systems Manager でオンプレミスリソースを管理およびモニタリングする** - AWS Systems Manager は、オンプレミスと AWS の両方でコンピューティングリソースを表示および制御するために使用できる AWS のサービスです。AWS Systems Manager コンソールを使用すると、すべてのマネージドインスタンスの運用データを表示し、マネージドリソース全体の運用タスクを自動化できます。AWS Systems Manager は、マネージドインスタンスをスキャンし、検出したポリシー違反についてレポートする (または修正アクションを実行する) ことで、セキュリティとコンプライアンスの維持を支援します。

  オンプレミスインフラストラクチャに AWS Systems Manager Agent (SSM Agent) をインストールし、AWS アカウントの AWS Systems Manager サービスに接続するように設定できます。SSM Agent は HTTPS ポート 443 経由で AWS のサービスと通信し、接続にインバウンドオープンポートを要求しません。

  Session Manager はフルマネージド型の AWS Systems Manager 機能であり、Amazon EC2 インスタンス、オンプレミスインスタンス (エッジゲートウェイなど)、仮想マシン (VM) を、インタラクティブなワンクリックのブラウザベースのシェルを使用するか、AWS CLI を使用して管理できます。Session Manager は、セキュアで監査可能なインスタンス管理を提供します。インバウ

ンドポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりする必要はありません。また、Session Manager では、インスタンスへの制御されたアクセス、厳格なセキュリティプラクティス、完全に監査可能なログ (インスタンスアクセスの詳細を含む) を必要とする企業ポリシーに簡単に準拠できます。同時に、エンドユーザーにはマネージドインスタンスへのシンプルなワンクリックのクロスプラットフォームアクセスを提供します。

- **AWS が提供するオンプレミスのインフラストラクチャソリューションを使用して管理とモニタリングをシンプルにする** - AWS では、AWS とオンプレミス環境全体で一貫したエクスペリエンスを実現するハイブリッドクラウド環境向けのソリューションを提供しています。AWS Outposts は、AWS クラウドをオンプレミス環境まで拡張するフルマネージド型のハイブリッドソリューションであり、AWS クラウドと同じ AWS インフラストラクチャ、サービス、API、管理ツール、サポート、運用モデルを提供します。AWS Outposts はクラウドからセキュアに管理できます。さまざまな従来のオンプレミス製造アプリケーション (SCADA/MES) やエッジアプリケーションを実行するために使用できます。AWS クラウドリソースと同様に、オンプレミスのリソースを管理およびアクセスするためのセキュアで一貫したエクスペリエンスを提供します。また、AWS のサービス (Amazon CloudWatch や AWS Systems Manager など) を簡単に活用して継続的なモニタリングや管理を行うこともできます。

  AWS Snow Family は、エッジでデータを収集して処理するためのセキュアで高いポータブルデバイスを提供します。オフラインで動作するように設計されており、ローカライズされた管理、モニタリング、タスクのオートメーションの各機能を AWS OpsHub アプリケーションで提供します。AWS Snow Family では、セキュリティグループ、ローカルの IAM ユーザー、ロール、ポリシーなどのセキュリティ機能も利用できます。これにより、お客様はコードを使用してセ

キュリティを実装できます。また、完全なクラウド環境での場合と同様の方法で許可を論じることができます。

- **IoT デバイスでは、AWS IoT Device Management のセキュアトンネリングを使用する** - IoT デバイスでは、セキュアトンネリングを使用し、AWS IoT が管理するセキュアな接続を介して、リモートデバイスへの双方向通信を確立できます。セキュアトンネリングを使用すると、既存のインバウンドファイアウォールルールを更新する必要がないため、お客様はファイアウォールルールが提供するセキュリティレベルをリモートサイトで維持できます。トンネルのアクセス許可は、IAM アクセス許可ポリシーを使用してクラウドで管理できるため、お客様は一貫した方法でアクセスを管理できます。

  例えば、数百マイル離れた工場にあるセンサーデバイスで、工場の温度測定に問題があるとします。セキュアトンネリングを使用すると、そのセンサーデバイスへのセッションを開いてすばやく開始できます。問題 (不正な設定ファイルなど) を特定すると、ファイルをリセットし、同じセッションを通じてセンサーデバイスを再起動できます。従来のトラブルシューティング (センサーデバイスを調査するために技術者を工場に派遣するなど) と比べて、セキュアトンネリングではインシデント対応の迅速化、復旧時間の短縮、運用コストの削減が可能になります。

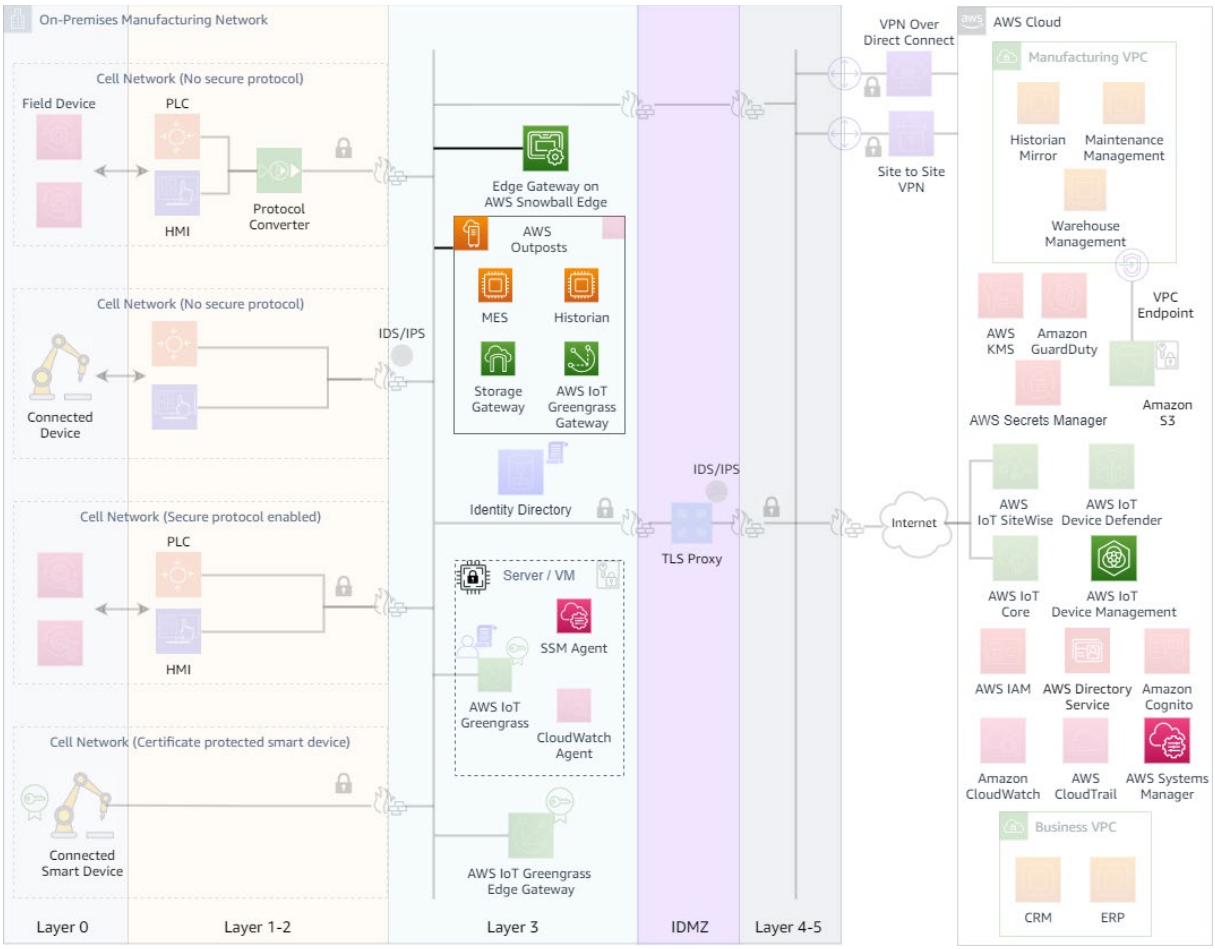

図 *12* - コンピューティングリソースのセキュアな管理とアクセス

ネットワークトラフィックおよびリソースを継続的にモニタリングする

セキュリティは、リソースのアーキテクチャ設計と設定を 1 回行えば済むというものではありません。ネットワークを長期にわたってセキュアに保つには、継続的なモニタリングを通じて変更や悪意のある行為を検出することが不可欠です。オートメーションはクラウドの重要な利点です。しきい値処理と修復のスクリプトを作成できるため、モニタリング > 検出 > アクションのサイクルを人間の介入なしで実行できます。また、モニタリングする対象には、ネットワークトラフィック、アプリケーションログ、オペレーティングシステムログなど、複数の情報ソースを包括的に含める必要があります

(クラウドを使用すると、セキュリティ分析を簡単に行うことができます)。 図 14 は、これらのベストプラクティスの一部を示しています。

- **デジタルアセットインベントリを維持し、ネットワークトラフィックをモニタリングおよび分析する** – セキュアな ICS ネットワークを維持するうえで重要な要素は、産業用ネットワーク内のハードウェアアセットとソフトウェアアセットの両方のインベントリを特定、維持、管理することです。ネットワーク化したアセットインベントリを確立したら、すべてのデバイス接続をマッピングするネットワークインタラクションベースラインを作成し、逸脱がないかどうかを継続的にモニタリングする必要があります。ローカルネットワークトラフィックは、ネットワーク分析を使用してモニタリングおよび分析する必要があります。

  専用の OT ネットワーク分析ツールを使用すると、ネットワークトラフィックを受動的にモニタリングすることで、ハードウェアアセットインベントリを作成できます。また、これらのツールは、産業用プロトコルを分析し、ネットワークデバイス間でやりとりされる特定のデータやコマンドに関する情報を提供することで、より深いインサイトを提供できます。ベースラインからの逸脱時にアラートを送信する自動ルールも設定する必要があります。専用ツールとは別に、Zeek などのオープンソースツールを使用すると、工場内のネットワークインタラクションの包括的なビューを取得する機能などを利用できます。AWS Systems Manager は、これらの機能を補完するために、マネージドリソースからソフトウェアインベントリを自動的に収集する方法を提供できます。

  AWS クラウドで Amazon GuardDuty を有効にして、脅威、悪意のある行為、不正な動作を継続的に検出します。Amazon GuardDuty は、機械学習、異常検出、統合された脅威インテリジェンスを使用することで、潜在的な脅威を特定して優先順位を付ける「ワンスイッチ」ショップです。Amazon GuardDuty は、AWS CloudTrail、VPC フローログ、DNS ログなど、複数の AWS データソースにわたる数百億件のイベントを分析します。Amazon CloudWatch Events

と統合することで、Amazon GuardDuty アラートをすぐ使用して、複数のアカウントにわたって簡単に集約し、既存のイベント管理システムやワークフローシステムに容易にプッシュできます。

- **ローカルアプリケーション、オペレーティングシステム、インフラストラクチャのログとメトリクスを収集する** - アプリケーション、オペレーティングシステム、インフラストラクチャのログとメトリクスは、セキュリティの脅威の管理と検出だけでなく、アプリケーションの問題のトラブルシューティングや早期アラートにも重要な情報ソースです。産業用制御システム (ICS: Industrial Control Systems) では、通常、これらのログはローカルに保持され、トラブルシューティング時にのみ分析されます。Amazon CloudWatch や Amazon Kinesis などの AWS のサービスを使用して、ログを一元的に収集できます。AWS Glue、Amazon EMR、Amazon OpenSearch Service などのサービスを使用して、ログデータを大規模に分析したり、検出した悪意のある行為について警告する自動ルールを作成したりできます。例えば、SCADA/MES システムのアプリケーションログとホストサーバーログは、Amazon CloudWatch エージェントを使用して収集し、検索と分析のために Amazon CloudWatch や Amazon OpenSearch Service に送信できます。Amazon CloudWatch のイベントとアラームを、異常な状態を検出するように設定することもできます。

  ハードウェア/サーバーのパフォーマンスメトリクスは悪意のある行為の指標 (CPU/ネットワーク使用率の急増など) となるため、継続的に収集、モニタリング、分析する必要があります。Amazon CloudWatch は、パフォーマンスメトリクスの収集とモニタリングに役立つ重要なサービスです。Amazon CloudWatch エージェントをオンプレミスサーバー/仮想マシンで使用して、メトリクスを直接収集できます。

  メトリクスとログは、エッジゲートウェイ経由でクラウドに転送することもできます。エッジゲートウェイはリアルタイムの分析と検出を行うように設定できる

ため、お客様はオンプレミスで脅威を検出できます。サードパーティーの AWS パートナーの製品を利用して、この方法で該当データを収集することもできます。

AWS が提供するソリューションをオンプレミスインフラストラクチャで使用すると、組み込みのメカニズムとクラウドサービスとの統合が深まり、このパフォーマンスとログのデータをさらに簡単に収集できます。例えば、AWS Outposts には、モニタリングと分析のために Amazon CloudWatch、AWS CloudTrail、VPC フローログとの統合が組み込まれています。

- **AWS IoT Device Defender を使用して IoT デバイスを監査およびモニタリングする** - AWS IoT Device Defender は、IoT デバイスのフリートの保護に役立つフルマネージドサービスです。AWS IoT Device Defender は IoT 設定を継続的に監査し、セキュリティのベストプラクティスから逸脱していないことを確認します。設定とは、デバイスが相互に通信したり、クラウドと通信したりする際に情報をセキュアに保つために設定する一連の技術的コントロールです。AWS IoT Device Defender を使用すると、デバイス ID の確認、デバイスの認証と認可、デバイスのデータ暗号化などの IoT 設定の維持と適用が容易になります。AWS IoT Device Defender は、事前定義済みの一連のセキュリティベストプラクティスに照らして、デバイスの IoT 設定を継続的に監査します (監査チェックの詳細なリストは AWS IoT Defender デベロッパーガイドに記載してあります)。AWS IoT Device Defender は、複数のデバイス間で ID 証明書を共有していたり、デバイスで失効した ID 証明書を使用して AWS IoT Core に接続しようとしたりするなど、セキュリティリスクを生じるような IoT 設定のギャップを検出すると、アラートを送信します。

  また、AWS IoT Device Defender は、デバイスや AWS IoT Core のセキュリティメトリクスを継続的にモニタリングして、デバイスごとに適切として定義されている動作との逸脱を確認することもできます。逸脱が発生すると、AWS

IoT Device Defender は問題の修正を促すアラートを送信します (図 13 を参照)。例えば、アウトバウンドトラフィックが急増した場合は、デバイスが DDoS 攻撃に参加している可能性があります。AWS IoT Greengrass と FreeRTOS は AWS IoT Device Defender と自動的に統合し、デバイスのセキュリティメトリクスを評価のために提供します。

AWS IoT Device Defender は、AWS IoT コンソール、Amazon CloudWatch、Amazon SNS にアラートを送信できます。AWS IoT Device Management を使用して、セキュリティ修正をプッシュするなど、アラートに基づく緩和アクションを実行できます。

re:Invent の「AWS のマルチレイヤーセキュリティアプローチで IoT セキュリティを強化する」を参照し、IoT 防御の原則に関する詳しい説明と、AWS IoT Device Defender 機能のデモンストレーションをご覧ください。

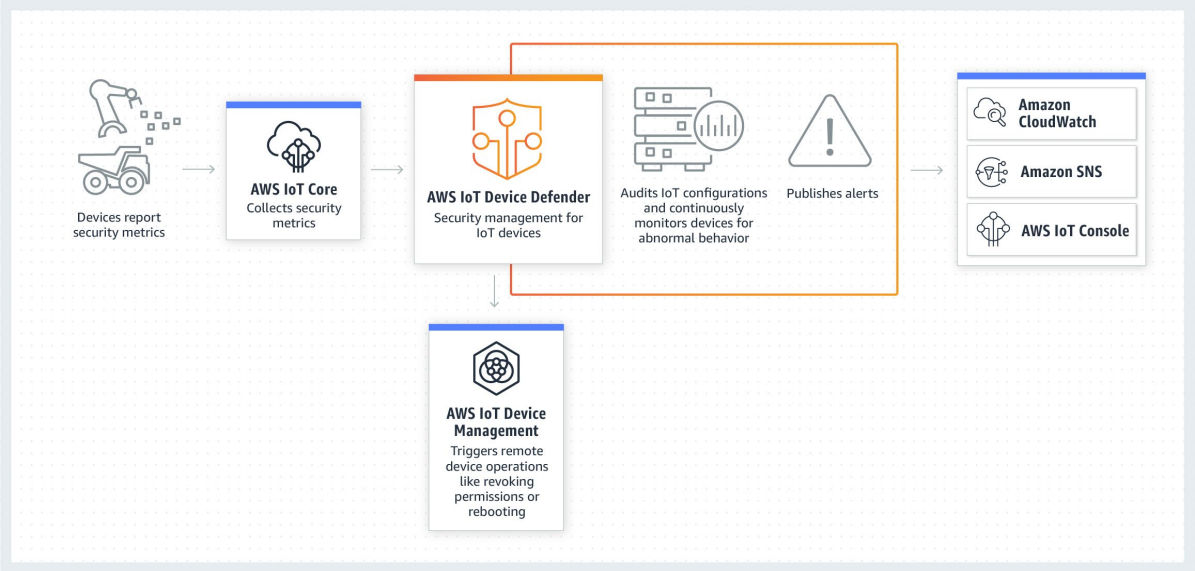

図 *13 - AWS IoT Device Defender*

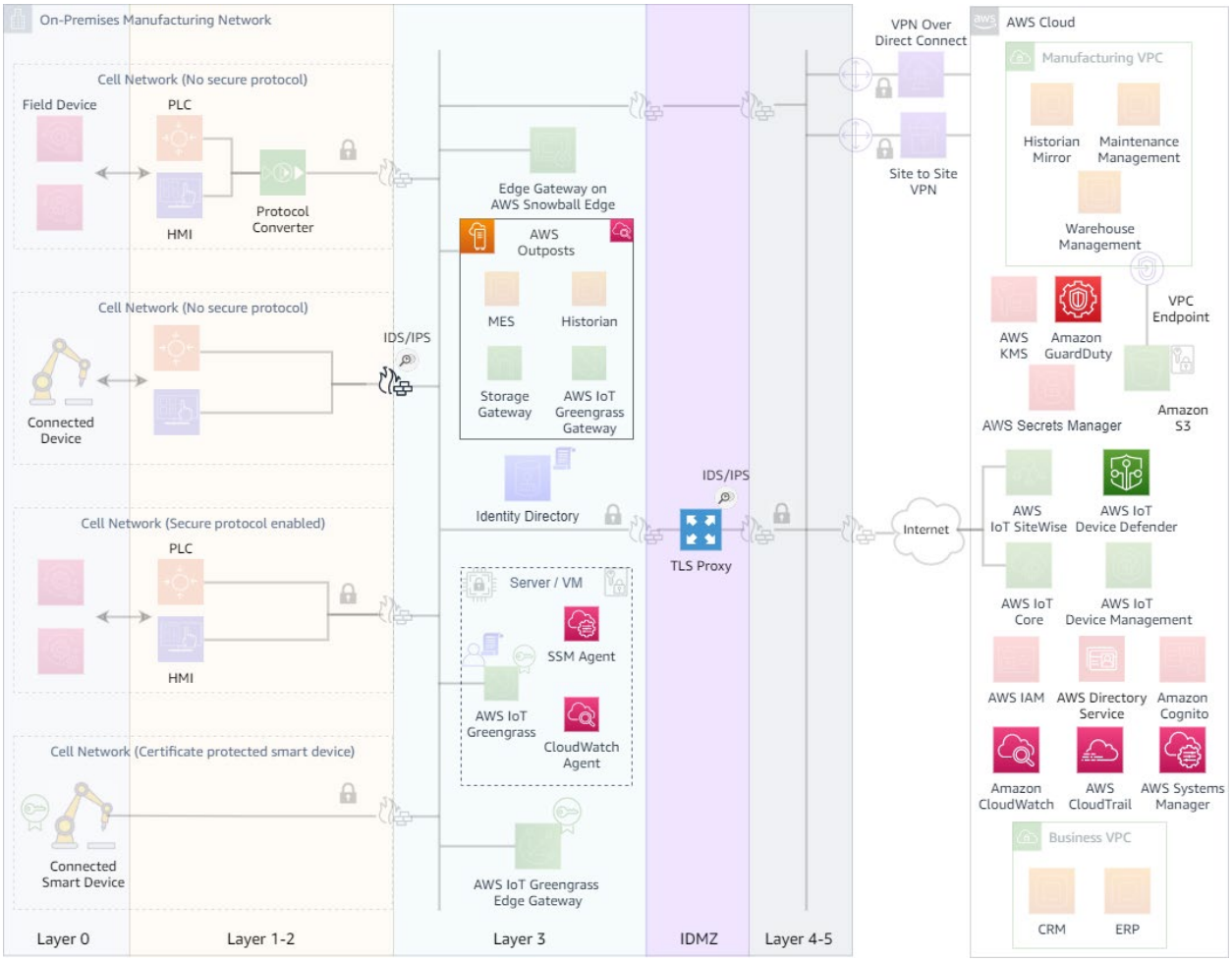

図 *14* - ネットワークトラフィックおよびリソースの継続的なモニタリング

製造データを保護する

製造データのセキュリティ確保と保護には、包括的なアプローチが必要です。OT およびクラウド環境内のデータを保護する重要な柱には、伝送中の暗号化、保管中の暗号化、アクセスコントロール、データ分類、データアクセスのモニタリング/監査があります。図 15 は、これらのベストプラクティスの一部を示しています。

- **伝送中および保管時のデータを暗号化する** - データフローパターンを調べて、伝送中のデータを確実に暗号化します。これまでのセクションで説明した、クラウドおよびネットワークリソースへの接続を保護するための推奨事項に従いま

す。ネットワークリソースにセキュアなプロトコルを使用し、できるだけ強力な暗号化を選択します。保管中のデータも確実に暗号化します。例えば、エッジゲートウェイなどのコンピューティングリソースでディスク暗号化を使用します。

クラウドリソースの暗号化の手法は、AWS のサービスごとに異なる場合があります。サービス別のドキュメントを参照し、伝送中と保管中の暗号化の設定が適切であることを確認してください。例えば、図 15 は、Amazon S3 バケットに保存したデータを保管中および伝送中に暗号化する方法を示しています。

- **最小権限の原則を使用してアクセスコントロールを適用し、データアクセスをモニタリング/監査する** - データソースとデータコンシューマーの両方で OT リソースのデータアクセスコントロールを適用します。データソースでは、アクセスコントロールをアプリケーション、OS、Active Directory のレベルで適用し、既知のエンティティへのアクセスを制限して、必要なリソースへのアクセスのみを許可する必要があります。また、データコンシューマーは固有の ID を使用して設定し、目的のデータソースに限定して通信とアクセスを許可する必要があります。データコンシューマーが AWS のサービス (Amazon Kinesis Streams、Amazon S3 バケット) である場合は、IAM のアクセスポリシーやリソースポリシーを使用できます。

  アクセスコントロールは、ファイアウォールやデータダイオード (単方向ネットワークデバイス) などのセキュリティアプライアンスを使用して接続レイヤーでも適用する必要があります。

  OT のアクセスコントロールを計画するときは、ネットワークリソースの物理的なセキュリティを考慮する必要があります。コンピューティングハードウェア、ネットワークインフラストラクチャ、セキュリティアプライアンスへの物理的なアクセスは、厳密に制御し、少数の承認された担当者にのみ制限する必要があります。

コンピューティングとストレージのライフサイクル終了を管理するための制御手段も考慮する必要があります。ライフサイクルの終了時に、NIST 媒体のデータ抹消処理 (サニタイズ) に関するガイドラインに従って、データを確実に抹消処理します。

本書で説明しているモニタリングのベストプラクティスのガイドラインに従い、データの使用状況とデータアクセスのモニタリングをモニタリング計画全体の一部として確実に組み込みます。モニタリングデータをリアルタイムで分析したり、アラートを送信したり、自動アクションを実行したりするように自動ルールを設定します。

クラウド内のリソースの場合、クラウド内のリソースの物理的なセキュリティは、責任共有モデルに従って AWS の責任となります。ただし、お客様は、クラウドへの接続と、クラウド内で実行するワークロードを保護する責任があります。AWS は、さまざまなアクセスコントロールやモニタリング/監査メカニズムを用意しており、お客様がクラウド内で実行しているワークロードを保護するのに役立ちます。これらのメカニズムはサービスごとに異なる場合があります。サービス別のドキュメントを参照し、クラウドリソースへのアクセスコントロールを適切に適用していることを確認してください。

- **エッジおよびエージェントソフトウェアのレジリエンシーの機能を使用して、リアルタイムのデータ損失を防ぐ** - データ損失防止も、データセキュリティにおいて考慮すべき重要な要素です。レジリエンシー (回復性) を念頭に置いてデータ収集を設計します。エッジおよびエージェントソフトウェアで「ストアアンドフォワード」などの機能を使用して、断続的なデータ損失から保護します。例えば、AWS IoT Greengrass はストリームマネージャーを提供し、断続的な接続が発生した場合にデータストリームをローカルに保存します。また、その他のレジリエンシーの機能として、AWS IoT Core との永続的なセッションやクラウドターゲットのメッセージキューなども提供しています。

- **バックアップとビジネス継続性のためにクラウドを使用する** - ローカルの産業用設備で有害事象が発生した場合でも、データやシステムを確実に利用できるようにするには、効果的なデータバックアップと災害対策の戦略が不可欠です。

  クラウドは、実質的に無制限の、耐久性と費用対効果に優れたストレージを提供するため、バックアップと復元のユースケースの魅力的なターゲットです。Amazon S3 と Amazon S3 Glacier は、バックアップデータを保存するための主要なターゲットです。これらは、バックアップデータを保存するための高い耐久性、柔軟性、スケーラビリティ、およびセキュリティに優れたサービスを提供します。多くのサードパーティーサービスには、クラウドにデータを送信するためのクラウドコネクタが組み込まれています。

  ビジネス継続性を確保するには、システム障害、サーバー障害、サイバー攻撃が発生した場合にシステムをどれほど迅速かつ効率的に復元できるかについて、より慎重に検討する必要があります。AWS では、AWS Elastic Disaster Recovery を使用すると、オンプレミスの物理サーバーと仮想サーバー、およびデータベースのダウンタイムとデータ損失を最小限に抑えることができます。CloudEndure は、AWS クラウド内でマシンを低コストのステージングエリアに継続的にレプリケートできます。また、フェイルオーバー後のオンプレミスへのフェイルバック機能も提供しています。

  製造においては、一部の低レイテンシーのワークロードは、中断期間が短くてもクラウド内で実行できなくなる場合があります。したがって、災害対策計画には、オンプレミスとのワークロードを別のオンプレミスインフラストラクチャ (AWS Snowball Edge や AWS Outposts など) で実行するための考慮事項を含める必要があります。

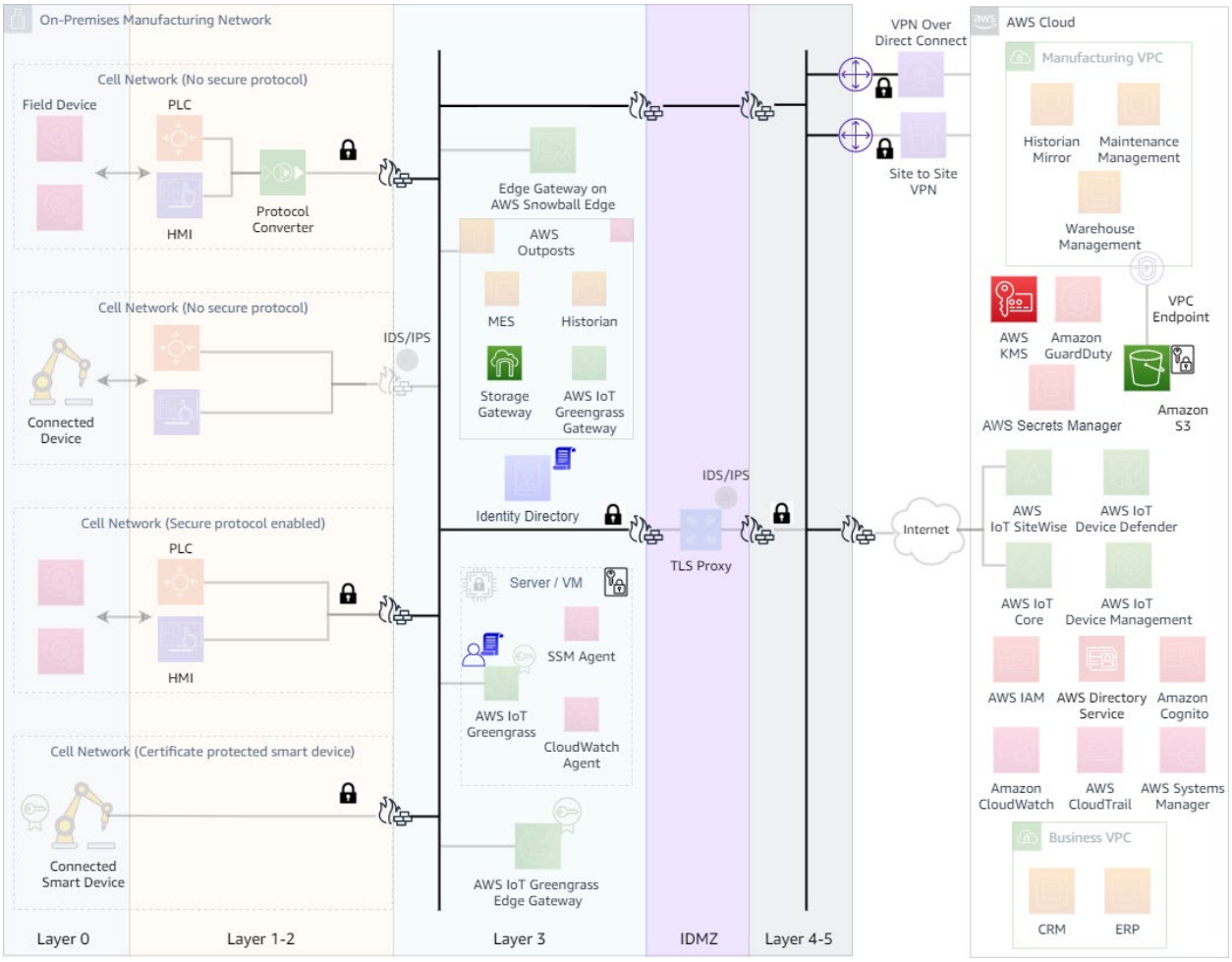

図 *15* - 製造データの保護

まとめ

要約すると、このドキュメントでは、AWS クラウドを使用してオンプレミスのハイブリッドワークロード向けに製造 OT 環境のアーキテクチャの設計および管理を行うためのベストプラクティスを紹介しました。最初に、業界標準の Purdue モデルを使用して従来のネットワークアーキテクチャを確認しました。次に、AWS Edge と AWS クラウドサービスが従来の運用モデルのモダナイゼーションにどのように役立つかを説明しました。シナリオでは一般的な使用パターンについて説明しました。IT/OT のコンバージェンスに伴って、どのような新しいセキュリティ上の課題が生じるかを説明

し、これらの新しい課題に対処するためのセキュリティの基本原則を確認しました。また、これらの特定の課題に対する規範的なガイダンスやベストプラクティスとして、クラウドへのネットワーク接続の確保、産業用のアセットや OT ネットワークリソースのセキュアなアクセス、管理、継続的なモニタリングなどについて説明しました。

寄稿者

この文書の寄稿者は次のとおりです。

- Nishant Saini (アマゾン ウェブ サービス、ソリューションアーキテクト)
- Russell de Pina (アマゾン ウェブ サービス、ソリューションアーキテクト)
- Ryan Dsouza (アマゾン ウェブ サービス、ソリューションアーキテクト)
- Bernard Paques (アマゾン ウェブ サービス、ソリューションアーキテクト)
- Steve Blackwell (アマゾン ウェブ サービス、製造、テクニカルリーダー)

参考資料

詳細については、次を参照してください。

- ハイブリッド接続に関するホワイトペーパー
- セキュリティの柱 - AWS Well-Architected フレームワーク
- IoT レンズ - AWS Well-Architected フレームワーク
- セキュリティ関連 NIST 文書 - Guide to Industrial Control System Security
- NIST ガイドライン - Zero Trust Architecture

ドキュメントの改訂

日付	説明
2021 年 5 月 20 日	初版発行